Please type a plus (+) inside this box → ⊞

3-16-00

A

PTO/SB/29 (12/97)
Approved for use through 09/30/00. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	9967-003-999	*Total Pages*	
First Named Inventor or Application Identifier			
Ken Xie			
Express Mail Label No.	EL 451 593 710 US		

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: **Assistant Commissioner for Patents**
Box Patent Application
Washington, DC 20231

1. ☒ Fee Transmittal Form [Total pages 2]
Submit an original, and a duplicate for fee processing)

2. ☒ Specification [*Total Pages* - 33]
(preferred arrangement set forth below) (Includes Appendix *A*)
-Descriptive title of the Invention
-Cross Reference to Related Applications
-Statement Regarding Fed sponsored R&D
-Reference to Microfiche Appendix
-Background of the Invention
-Brief Summary of the Invention
-Brief Description of the Drawings *(if filed)*
-Detailed Description of the Invention (including drawings, *if filed*)
-Claim(s)
-Abstract of the Disclosure

3. ☒ Drawing(s) *(35 USC 113)* [*Total Sheets* 7]

4. ☒ Oath or Declaration [*Total Sheets* 2]
a. ☒ Newly executed (original or copy)
b. □ Copy from a prior application (37 CFR 1.63(d))
(for continuation/divisional with Box 17 completed)
[Note Box 5 below]
i. □ DELETION OF INVENTORS(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33 (b).

5. □ Incorporation By Reference *(useable if Box 4b is checked)*
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. □ Microfiche Computer Program *(Appendix)*

7. □ Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. □ Computer Readable Copy
b. □ Paper Copy (identical to computer copy)
c. □ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. ☒ Assignment Papers (cover sheet & document(s)) 3 pgs.
9. □ 37 CFR 3.73(b) Statement □ Power of Attorney
(when there is an assignee)
10. □ English Translation Document *(if applicable)*
11. □ Information Disclosure Statement (IDS)/PTO-1449 □ Copies of IDS Citations
12. □ Preliminary Amendment
13. ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
14. ☒ Small Entity Statement(s) [2 pages]
15. □ Certified Copy of Priority Document(s)
(if foreign priority is claimed)
16. □ Other:

17. **If a CONTINUING APPLICATION,** *check appropriate box and supply the requisite information:*
□ Continuation □ Divisional ☒ Continuation-in-part (CIP) of prior application No: 09/283,730 filed April 1, 1999.

18. CORRESPONDENCE ADDRESS

☒ Customer Number or Bar Code Label 20583 *(Insert Customer No. or Attach bar code label here)* or □ Correspondence address below

NAME					
ADDRESS					
CITY		*STATE*		*ZIP CODE*	
COUNTRY		*TELEPHONE*		*FAX*	

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: ☒ Application of: Ken Xie *et al.*
□ Patent of:

☒ Application No.: To be assigned
□ Patent No.:

Group Art Unit: To be assigned

☒ Filed: Herewith
□ Issued:

Examiner: To be assigned

For: A METHOD, APPARATUS, AND COMPUTER PROGRAM PRODUCT FOR A NETWORK FIREWALL

Attorney Docket No.: 9967-003-999

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS
[37 CFR 1.9(f) and 1.27(c)] - Small Business Concern

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

I hereby declare that I am

□ the owner of the small business concern identified below:
☒ an official of the small business concern empowered to act in behalf of the concern identified below:

Name of organization NetScreen Technologies, Inc.
Address of organization 2860 San Tomas Expressway
Santa Clara, CA 95051

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 37 CFR 1.9(d), for purposes of paying reduced fees under section 41(a) and (b) of Title 35, United States Code, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the person employed on a full-time, part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern and/or there is an obligation under contract or law by the inventor(s) to convey rights to the small business concern with regard to the invention entitled by inventor(s) Ken Xie et al. described in

□ the specification filed herewith
☒ application no. To be assigned filed Herewith
□ patent no. issued

If the rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights to the invention is listed below and no rights to the invention are held by any person, other than the inventor, who could not qualify as an independent inventor under 37 CFR 1.9(c) if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d), or a nonprofit organization under 37 CFR 1.9(e).

FULL NAME__________________________
ADDRESS__________________________

□ INDIVIDUAL □ SMALL BUSINESS CONCERN □ NONPROFIT ORGANIZATION

FULL NAME__________________________
ADDRESS__________________________

□ INDIVIDUAL □ SMALL BUSINESS CONCERN □ NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. [37 CFR 1.28 (b)]

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, and patent issuing thereon, or any patent to which this verified statement is directed.

Send correspondence to:

PENNIE & EDMONDS LLP
1155 Avenue of the Americas
New York, N.Y. 10036-2711

Direct Telephone calls to:
PENNIE & EDMONDS LLP
(212) 790-9090

Name of person signing Feng Deng
Title of person other than owner Vice President, Engineering
Address of person signing NetScreen Technologies, Inc.
2860 San Tomas Expressway
Santa Clara, CA 95051

Signature ________ Date 3/10/00

*NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities.

A METHOD, APPARATUS AND COMPUTER PROGRAM PRODUCT FOR A NETWORK FIREWALL

Ken Xie
Yan Ke
Yuming Mao

RELATED APPLICATIONS

The present application is a continuation-in-part of co-pending application serial no. 09/283,730.

FIELD OF THE INVENTION

The present invention relates to the field of computer networks. In particular, the present invention relates to a method, apparatus and computer program product for providing network security.

BACKGROUND OF THE INVENTION

A packet switch communication system includes a network of one or more routers connecting a plurality of users. A packet is the fundamental unit of transfer in the packet switch communication system. A user can be an individual user terminal or another network. A router is a switching device that receives packets containing data or control information on one port and, based on destination information contained within the packets, routes the packets out another port to their final destination, or to some intermediary destination(s). Conventional routers perform this switching function by evaluating header information contained within the packet in order to determine the proper output port for a particular packet.

As known, a communications network can be a public network, such as the Internet, in which data packets are passed between users over untrusted, i.e., non-secure communication links. Alternatively, various organizations, typically corporations, use what is known as an intranet communications network, accessible only by the organization's members, employees, or others having access authorization. Intranets typically connect one or more private servers, such as a local area network (LAN). The network configuration in a preferred embodiment of this invention can include a combination of public and private networks. For example, two or more LANs can be coupled together with individual terminals using a public network, such as the Internet. A network point that acts as an entrance to another network is known in the art as a gateway.

Conventional packet switched communication systems that include links between public and private networks typically include means to safeguard the private networks against intrusions through the gateway provided at the interface of the private and public networks. The means designed to prevent unauthorized access to or from a private are commonly known as firewalls, which can be implemented in both hardware and software, or a combination of both. Thus, a firewall is a device that can be coupled in-line between a public network and a private network for screening packets received from the public network.

Referring to Figure 1, a conventional packet switch communication system 100 can include two (or more) private networks 102a and 102b coupled by a public network 104 for facilitating the communication between a plurality of user terminals 106. Each private network 102 can include one or more servers and a plurality of individual terminals. Each private network 102 can be an intranet, such as a LAN. Public network 104 can be the Internet, or other public network having untrusted links for linking packets between private networks 102a and 102b. In a preferred embodiment, at each gateway between a private network 102 and public network 104 there is a firewall 110.

The architecture of an illustrative prior art firewall is shown in Fig. 2a. The firewall 110 generally includes one or more public network links 120, one or more private network links 122, and memory controller 124 coupled to the network links by a PCI bus 125. Memory controller 124 is also coupled by a memory bus 129 to a memory (RAM) 126 and a firewall engine, implemented in a preferred embodiment as an ASIC 128. The firewall engine ASIC 128 performs packet screening prior to routing packets through to private network 102. The firewall engine ASIC 128 processes the packets to enforce an access control policy, screening the packets in accordance with one or more sets of rules. The rules are described in more detail below. A central processor (CPU) 134 is coupled to memory controller 124 by a CPU bus 132. CPU 134 oversees the memory transfer operations on all buses shown. Memory controller 124 is a bridge connecting CPU bus 132, memory bus 129, and PCI bus 125.

In operation, packets are received at public network link 120. Each packet is transferred on bus 125 to, and routed through, memory controller 124 and on to RAM 126 via memory bus 129. When firewall engine 128 is available, packets are fetched using memory bus 129 and processed by the firewall engine 128. After processing, the packet is returned to RAM 126 using memory bus 129. Finally the packet is retrieved by the memory controller 124 using memory bus 129, and routed to private network link 122. The screening rules implemented by the firewall engine 128 are typically searched in linear order, beginning with the internal rule memory. Certain aspects of the rule structure are described below.

As known in the art, a rule is a control policy for filtering incoming and outgoing packets. Rules specify actions to be applied as against certain packets. When a packet is received for processing through a rule search, the packet's IP header, TCP header, or UDP header may require inspecting. A rule will generally include, at a minimum, source/destination IP addresses, UDP/TCP source/destination ports and transport layer protocol. Additional criteria may be used by the rules as well.

Generally, the address information is used as matching criterion – in other words to match a rule, a packet must have come from a defined source IP address and its destination must be the defined destination IP address. The UDP/TCP source/destination port specifies what client or server process the packet originates from on the source machine. The firewall engine can be configured to permit or deny a packet based upon these port numbers. The rule may include a range of values or a specific value for a TCP/UDP port. The transport layer protocol specifies which protocol above the IP layer, such as TCP or UDP, the policy rule is to be enforced against.

The firewall engine described above essentially screens packets using an access control list (ACL), and may be referred to as an ACL engine. That is, it performs a simple comparison of various matching criteria of an incoming IP packet – typically source, destination, port and protocol – to each rule in a rule set in sequence. Based upon this comparison, an incoming IP packet is either allowed or denied. A data-flow chart for this firewall engine is shown in Figure 5.

It will be appreciated that using a fixed set of rules can be restrictive in many practical applications. Therefore, it is desirable to provide a system and method capable of adding rules to the rule set of the firewall engine dynamically – that is, to extract from a sequence of packets information, such as the port number and IP address, and generate new rules using this information. However, generating these new rules dynamically would increase the complexity of the comparison and decrease the speed of the firewall engine. There is therefore a need in the art for a firewall engine which can generate rules dynamically, based upon information extracted from incoming packets, with a limited impact on the speed of the firewall engine.

SUMMARY OF THE INVENTION

In accordance with a preferred embodiment, an apparatus, method and computer program product for providing network security is described. The apparatus includes an engine for sorting incoming IP packets into initially allowed and initially denied packets using a fixed set of rules. The packets are then further sorted by a second engine. In one embodiment, the engine further sorts the initially denied packets into allowed packets and denied packets, using dynamically generated rules. The denied packets are dropped and the allowed packets are permitted to enter the network.

Likewise, the method includes the step of sorting incoming IP packets into initially allowed and initially denied packets using a fixed set of rules. The packets are then further sorted. In one embodiment, additional steps include sorting the initially denied packets into allowed packets and denied packets, using dynamically generated rules. The denied packets are dropped and the allowed packets are permitted to enter the network.

Finally, the computer program product sorts incoming IP packets into initially allowed packets and initially denied packets. In one embodiment, the computer program product further sorts the initially denied packets into allowed packets and denied packets, using dynamically generated rules. The denied packets are dropped and the allowed packets are permitted to enter the network.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates an exemplary packet switch communications system.

Figure 2a illustrates a firewall with an application-specific integrated circuit (ASIC).

Figure 2b illustrates a firewall with a local bus and an application-specific integrated circuit (ASIC).

Figure 3 illustrates an exemplary rule structure for use by a firewall.

Figure 4 is a flow diagram for a firewall screening process.

Figure 5 is a data-flow chart for a prior art firewall.

Figure 6 is a data-flow chart for a firewall in accordance with one embodiment of the invention.

Figure 7a is a logic diagram for processing incoming packets in accordance with the invention.

Figure 7b is a logic diagram for processing outgoing packets in accordance with the invention.

DETAILED DESCRIPTION OF THE INVENTION

A conventional firewall may be implemented in software, or in hardware as shown in Figure 2a. Alternatively, a hybrid of software and hardware may also be used to implement a firewall. The firewall of Figure 2a uses a memory bus 129 to communicate between the ASIC 128, the RAM 126, and the memory 130, which stores the rules used by the firewall. Figure 2b shows a high-speed firewall that employs a local bus 202 for improved processing speed. A high-speed firewall is described in pending parent application serial no. 09/283,730, the contents of which is hereby incorporated by reference. Exemplary high-speed firewalls include NetScreen Technology, Inc.'s integrated firewall products, described at www.netscreen.com and related web pages. Selected web pages describing NetScreen's high-speed firewalls are provided as Appendix A to this application.

As shown in Figure 2b, the high-speed firewall includes a hardware ASIC 204 to implement the firewall engine. The firewall engine retrieves packets stored in memory and processes each packet to enforce an access control policy. The processing by the firewall engine includes retrieving rules from a rule set, and screening the packets in accordance with the retrieved rules. In a specific embodiment, the rules may be stored in an internal memory in the ASIC 204, or may be retrieved from a separate rule memory 206 via the local bus 202. In a preferred embodiment, frequently accessed rule sets may be stored in the internal memory, with less-frequently accessed rule sets being stored in the separate rule memory 206.

The structure 500 of a rule used by a firewall engine in accordance with one embodiment of the present invention is shown in Figure 3. A rule will generally include, at a minimum, source/destination IP addresses 502 503, UDP/TCP source/destination ports 504 505 and transport layer protocol 510. Additional information used by the rules may include: a range of values for the UDP/TCP source/destination port 504 505; a counter 506 to keep track of the number of times the rule has been matched; a general mask (GMASK) 511 to indicate whether to ignore or check certain information in the packet header; source/destination IP address mask 508 to indicate whether to ignore part of an IP address, typically a specified number of the least significant bits; a searching control field 512 to tell the firewall engine to search in the separate rule memory 206 and to give a starting address; and a response action field 514 to specify the action to be taken if the rule is matched.

The address information is used as matching criterion – to match a rule, a packet must have come from the defined source IP address 502 and its destination must be the defined destination IP address 503. Part of the address may be masked using the source/destination IP address mask 508. The UDP/TCP source/destination port 504 505 specifies what client or server process the packet originates from on the source machine. The firewall engine can be configured to permit or deny a packet based upon these port numbers. The rule may include a range of values or a specific value for a

TCP/UDP port. The counter 506 is used to track the number of times a rule has been matched, and at some threshold value will trigger a certain action, such as deny, log or alarm. The transport layer protocol 510 specifies which protocol above the IP layer, such as TCP or UDP, the policy rule is to be enforced against.

Referring to Figures 2b and 4, a process 600 executed by the firewall engine in the ASIC 204 is shown for screening packets using both the on-chip and off-chip rule memories. The firewall engine process begins at step 602. A packet is received at an interface (public network interface 122) and transferred to dual-ported memory 203 using a DMA process executed by memory controller 124 (604).

CPU 134 reads the packet header information from packet memory and writes the packet information into special registers on ASIC 204 (606). These registers are mapped onto the system memory space, so CPU 134 has direct access to them. In an exemplary hardware firewall, the registers include: a source IP register; a destination IP register; a port register; a protocol register; and an acknowledge register, for storing the acknowledge bit from the packet.

CPU 134 also specifies which rule set to search by writing to a rule set specifier register (608). CPU 134 issues a command to the firewall engine located in the ASIC 204 by writing to a control register to initiate the ASIC rule search (610). Alternatively, the firewall engine may first check a stored look-up table with criteria relating to ongoing current applications or services, before searching the rules. In that case, the firewall engine first compares the contents of the special registers to the contents of a look-up table, where the look-up table includes the IP address, port and protocol corresponding to each current application or service. For example, if the packet is an FTP packet for an FTP that is ongoing, this information will be in the look-up table. If, on the other hand, the packet is an FTP packet for a newly-initiated FTP, the information will not be in the look-up table.

If the information is not in the look-up table, or if a look-up table is not used, the firewall engine then compares the contents of the special registers to each rule in sequence (611) until a match is found (612). The search stops when a match is found (613). Alternatively, for certain rules, known as counter rules, the firewall engine will increment the count register and continue the search. If the count threshold is exceeded, or if the search locates a match for a non-counter rule, the search results are written to a status register 616. Likewise, if no match is found, and the entire set of rules has been examined, the search results are written to the status register. In addition, when a match is found, if a look-up table is used the information identifying the current application, such as the IP address, port and protocol, are written to the look-up table so that later packets in the current application may be processed using the look-up table instead of a rule search.

During the search, CPU 134 polls the status register to check whether the firewall engine is busy or has completed the search. When the CPU 134 determines that the search is complete, the CPU 134 executes certain actions against the current packet based on the information in the status register, such as permit or deny the packet, signal an alarm, and log the packet.

The process described above is a prior art one-pass search process, as illustrated in Figure 5: the ACL engine 621 conducts a search through an optional look-up table, and then through rules, as illustrated in Figure 4, to determine whether a given packet matches a rule in the set and take action on that basis. The rules use a set of matching criteria – for example, source and destination IP address, and port number, indicating the application. These rules are fixed and use known matching criteria. The ACL engine 621 then allows some packets 622, and denies or drops, others 623.

As shown in Figure 6, in a preferred embodiment, the IP packets 620 enter the ACL engine 621. As in the prior art, the ACL engine 621 conducts a search, using fixed rules. The ACL engine then outputs allowed packets 632, and initially denied packets 633.

Unlike the prior art, the firewall engine that embodies one aspect of the present invention includes additional dynamic filtering, which further processes the packets. In particular, the initially denied packets 633 are processed by a dynamic filter 637, which allows some of the initially denied packets to pass through the firewall and enter the private network. The dynamic filter 637 conducts a search through an additional set of rules, which are dynamically generated. The dynamic filter 637 generates rules using criteria such as port number and IP address, which are extracted from incoming packets for applications, such as RealAudio, Netmeeting (which uses the H3232 protocol) and network file system (NFS).

For example, when an FTP is initiated, the first sequence of FTP packets, which includes information on the port number and the IP address, will be passed by the rules in the ACL engine 621. The dynamic filter 637 then extracts port number and IP address from this first sequence of packets, and generates new rules, similar to the fixed rules used by the ACL, including these criteria. Later sequences of FTP packets will be denied by the ACL engine 621, but the dynamic filter 637 will pass the packets based on the new, dynamically-generated rules. The way in which the search through the dynamically-generated rules is conducted is similar to the approach used in the ACL engine 621. The dynamic filter then drops packets which are finally denied 636, and allows other initially denied packets, which meet the additional access control requirements, to pass 635 through the firewall and enter the private network.

This approach to processing the incoming IP packets has advantages over the prior art. Using dynamically-generated rules allows for more flexible access policy. However, if dynamic rule generation was included in the ACL engine 621, the processing speed would be decreased. The dynamic filter 637 used in accordance with the present invention, following the ACL engine 621, advantageously allows the use of dynamically-generated rules, without increasing the processing time for those IP packets, which are initially allowed 632 by the ACL engine 621 based on the fixed rule set.

Another preferred embodiment, as shown in Figure 6, additionally allows for network address translation (NAT), to enable IP addresses, port numbers and message authentication codes (MACs) in the private network to be concealed from the public network. The public network can only access this information for the firewall. Thus, the destination information in the headers in the incoming packets must be changed, to reflect the private network IP addresses, port numbers and MAC. Furthermore, source information in the headers of outgoing packets must also be changed, to reflect the firewall network IP address, port number and MAC.

However, depending on the particular application used, information relating to the IP address or port number may be embedded in the packet content or payload, as well as in the header. In that case, the packet payload for an incoming packet must be translated to reflect the internal IP address and port number, as shown in Figure 7a.

Likewise, the packet payload for an outgoing packet must be translated to reflect the firewall address and port number, as shown in Figure 7b.

As shown in Figure 6, the dynamic analyzer 638 examines those packets which are initially allowed 632 by the ACL engine 621. The dynamic analyzer 638 determines whether a given packet may require modification, due to embedded address or port number information. The dynamic analyzer 638 then separates packets which may require modification 640 from packets which do not require modification 639. Packets which include IP address or port number information are identified by reading a protocol-specific field in the header. The dynamic analyzer 638 allows those initially allowed packets 632 and 635 which do not require modification 639 to pass through the firewall 642 into the private network.

The packets 640 which may require modification are then passed to an application-specific handler 641. The application-specific handler 641, as its name suggests, processes packets 640 for a particular application, such as FTP or NFS. The application-specific handler examines the protocol, session, port number and IP address, as well as the payload. In one embodiment, the application-specific handler may modify certain packets, which have been allowed 632 and 635. If the IP address or port number in the packet header have been changed, for an incoming packet, or must be changed, for an outgoing packet, the application-specific handler translates the payload to reflect the change. In another embodiment, multiple application-specific handlers 641 may be provided, to process packets for different applications. For example, the firewall may include both an FTP-specific handler and an NFS-specific handler.

In another embodiment, the application-specific handler 641 may include the capability to send a "reset" packet to inform the TCP processor sending the denied packets that the connection has been denied. The connection is thereby rejected, rather than merely dropped. The rejection will prevent the TCP processor sending the denied packets 636 from continuing to try to connect with the network, thereby avoiding wasted bandwidth.

In conjunction with the software functionality description provided in the present disclosure, an apparatus in accordance with the preferred embodiments may be programmed using methods known in the art as described, for example, in Francise et.

al., *Professional Active Server Pages 2.0*, Wrox Press (1998), and Zaration, *Microsoft C++ 6.0 Programmer's Guide*, Microsoft Press (1998), the contents of each of which is hereby incorporated by reference into the present application.

While preferred embodiments of the invention have been described, these descriptions are merely illustrative and are not intended to limit the present invention. For example, while the preferred embodiment discusses primarily a hardware implementation of a firewall, the scope of the preferred embodiments is not so limited. Those skilled in the art will recognize that the disclosed software and methods are readily adaptable for broader network analysis applications.

CLAIMS

What is claimed is:

1. An apparatus for providing a computer security firewall, comprising:

an ASIC including a firewall engine with a first engine including a first set of rules for sorting incoming IP packets into initially allowed packets and initially denied packets, and a filter including a second set of rules for receiving and further sorting the initially denied packets into allowed packets and denied packets.

2. The apparatus of claim 1, wherein the filter dynamically generates the second set of rules.

3. The apparatus of claim 2, wherein the first set of rules comprises fixed rules.

4. The apparatus of claim 3, further comprising:

a second engine for receiving and further processing the initially allowed packets.

5. The apparatus of claim 4, wherein the second engine is capable of modifying some subset of the initially allowed packets.

6. The apparatus of claim 5, wherein the second engine comprises a dynamic analyzer for identifying initially allowed packets requiring network address translation, and a handler for providing network address translation.

7. The apparatus of claim 5, wherein the second engine comprises a dynamic analyzer for sending a "reset" packet to a source IP address.

8. A computer software product for providing a network security firewall, comprising:

computer code for sorting incoming IP packets into initially allowed packets and initially denied packets;

computer code for extracting matching criteria from incoming IP packets;

computer code for dynamically generating rules using the extracted matching criteria; and

computer code for further sorting the initially denied packets using the dynamically-generated rules.

9. The computer software product of claim 8, wherein the computer code for sorting incoming IP packets uses fixed rules.

10. The computer software product of claim 9, further comprising:

computer code for further sorting the initially allowed packets into allowed packets and packets requiring modification.

11. The computer software product of claim 10, further comprising computer code for modifying control packets.

12. The computer software product of claim 11, wherein the computer code for modifying control packets includes computer code for network address translation.

13. The computer software product of claim 10, further comprising:

computer code for generating and transmitting a "reset" packet in response to a denied packet.

14. A method for providing network computer security, comprising:

receiving incoming IP packets at a firewall;

sorting the incoming IP packets into initially allowed packets and initially denied packets; and

further sorting the initially denied packets into allowed and denied packets using dynamically-generated rules.

15. The method of claim 14, wherein the step of sorting the incoming IP packets is performed using fixed rules.

16. The method of claim 15, further comprising the step of further sorting the initially allowed packets into allowed packets and packets requiring modification.

17. The method of claim 16, further comprising the step of providing network address translation for packets requiring modification.

18. A method for providing network computer security, comprising:

receiving incoming IP packets at a firewall;

sorting the incoming IP packets into initially allowed packets and initially denied packets using a set of fixed rules;

extracting parameters from the incoming IP packets;

using the extracted parameters to generate a set of dynamically-generated rules; and

further sorting the initially denied packets into allowed and denied packets using the dynamically-generated rules.

19. The method of claim 18, further comprising the step of further sorting the initially allowed packets into allowed packets and packets requiring modification.

20. The method of claim 19, further comprising the step of providing network address translation for packets requiring modification.

ABSTRACT

An improved firewall for providing network security is described. The improved firewall provides for dynamic rule generation, as well using conventional fixed rules. This improvement is provided without significant increase in the processing time required for most packets. Additionally, the improved firewall provides for translation of IP addresses between the firewall and the internal network.

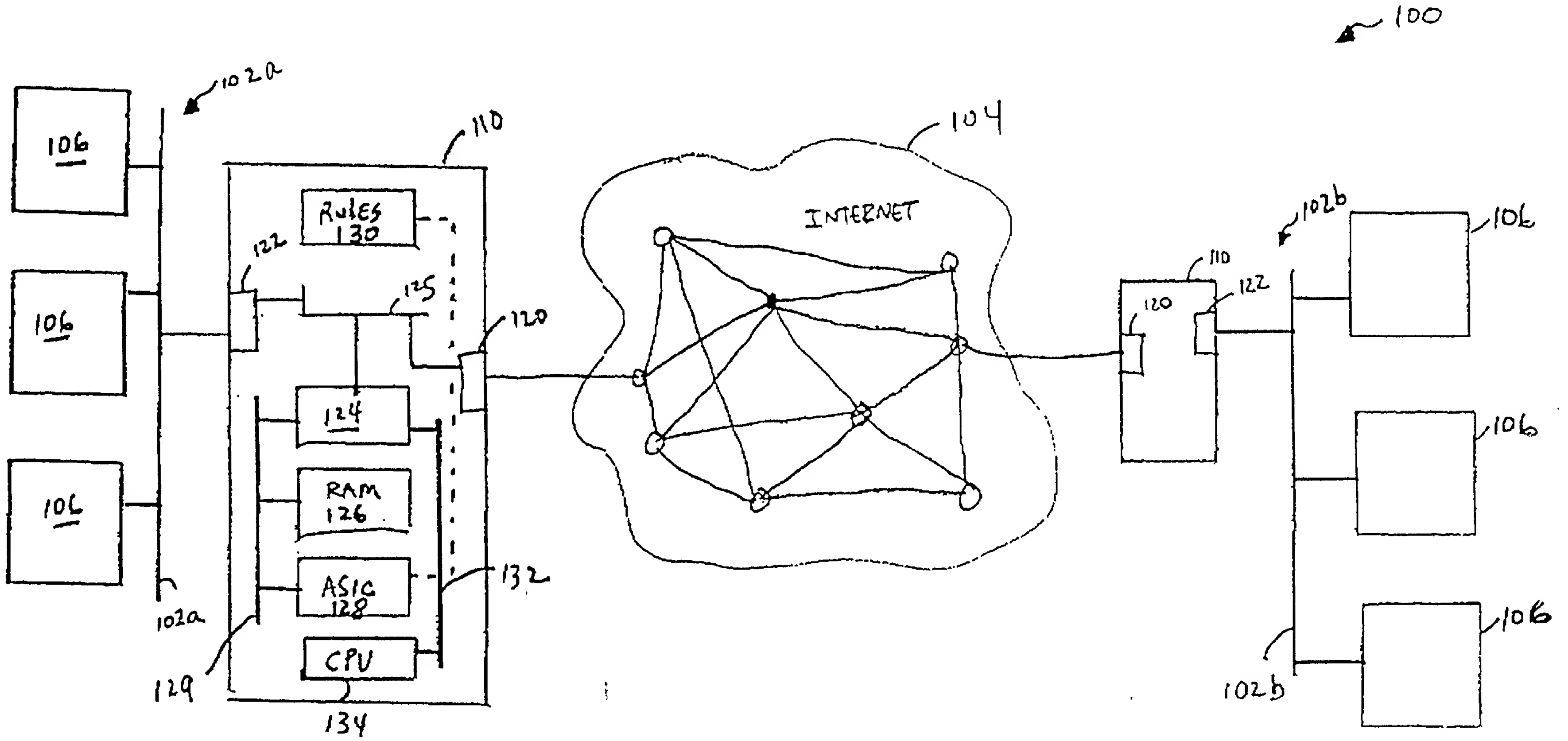
100
106
106
106
102a
102a
110
Rules
130
122
125
120
124
RAM
126
ASIC
128
CPU
129
132
134
104
INTERNET
110
120
122
102b
102b
106
106
106

Fig. 1

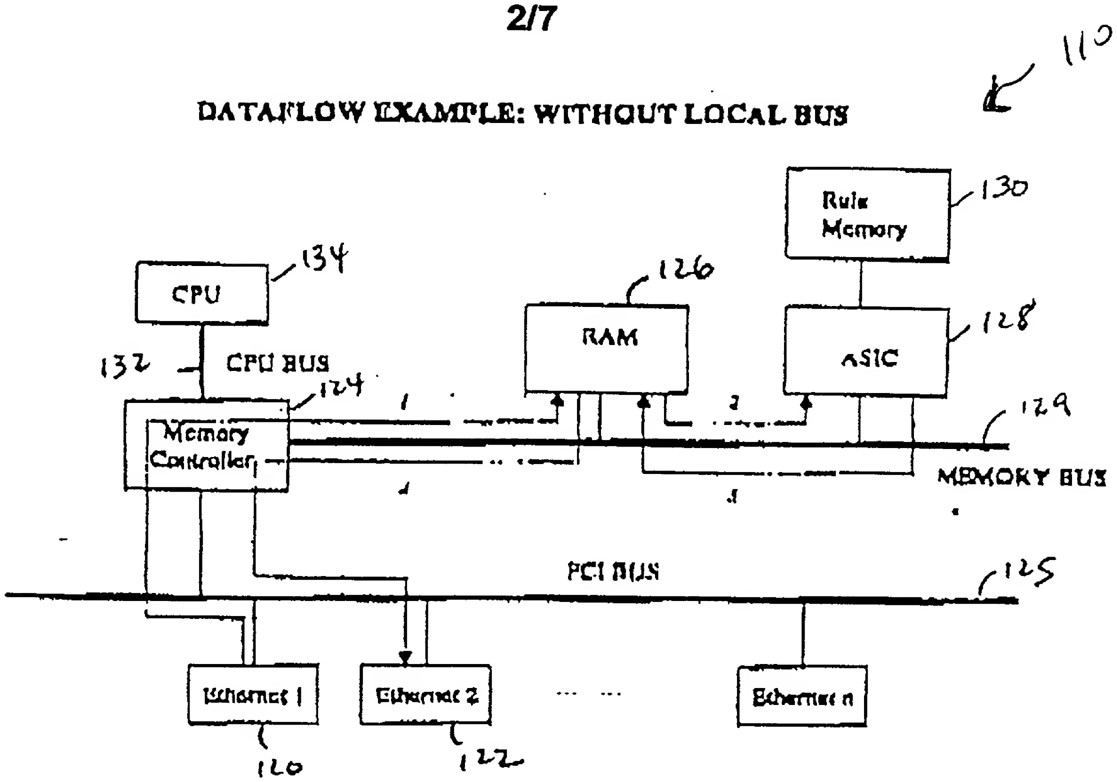
110
DATAFLOW EXAMPLE: WITHOUT LOCAL BUS
Rule Memory
130
CPU
134
RAM
126
ASIC
128
132
CPU BUS
124
Memory Controller
1
2
129
MEMORY BUS
4
3
PCI BUS
125
Ethernet 1
Ethernet 2
... ...
Ethernet n
120
122

FIG. 2a

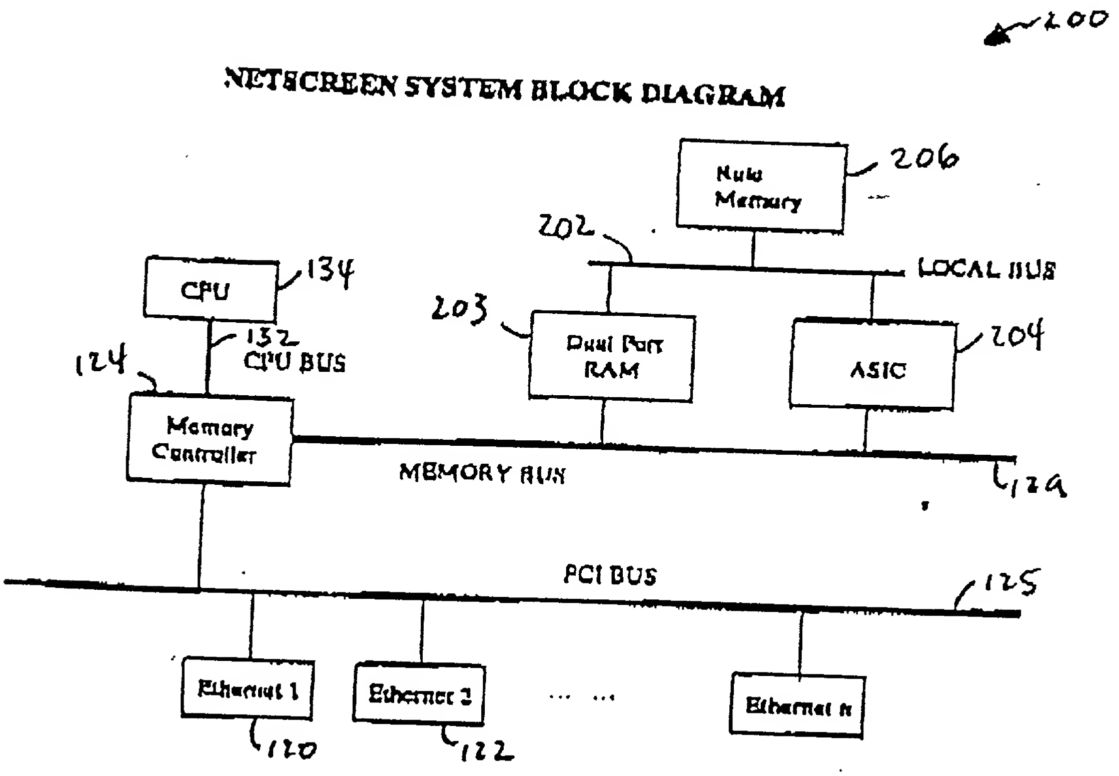
200
NETSCREEN SYSTEM BLOCK DIAGRAM
Rule Memory
206
202
LOCAL BUS
CPU
134
203
Dual Port RAM
ASIC
204
124
132
CPU BUS
Memory Controller
MEMORY BUS
129
PCI BUS
125
Ethernet 1
Ethernet 2
... ...
Ethernet n
120
122

FIG. 2b

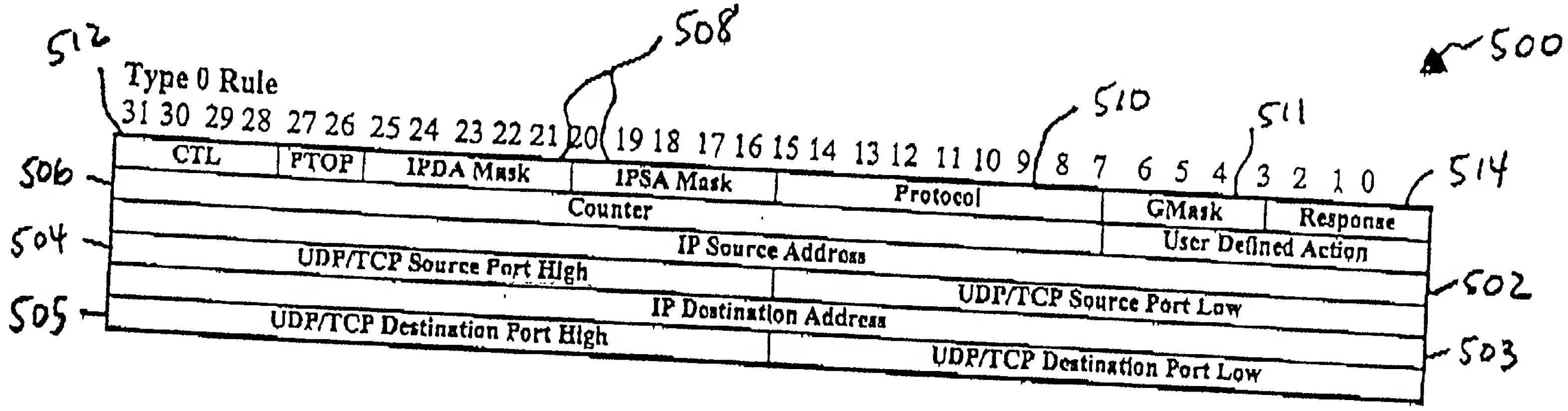
500
512
Type 0 Rule
31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
508
510
511
514
CTL
PTOP
IPDA Mask
IPSA Mask
Protocol
GMask
Response
506
Counter
User Defined Action
504
IP Source Address
UDP/TCP Source Port High
UDP/TCP Source Port Low
502
505
IP Destination Address
UDP/TCP Destination Port High
UDP/TCP Destination Port Low
503

FIG.3

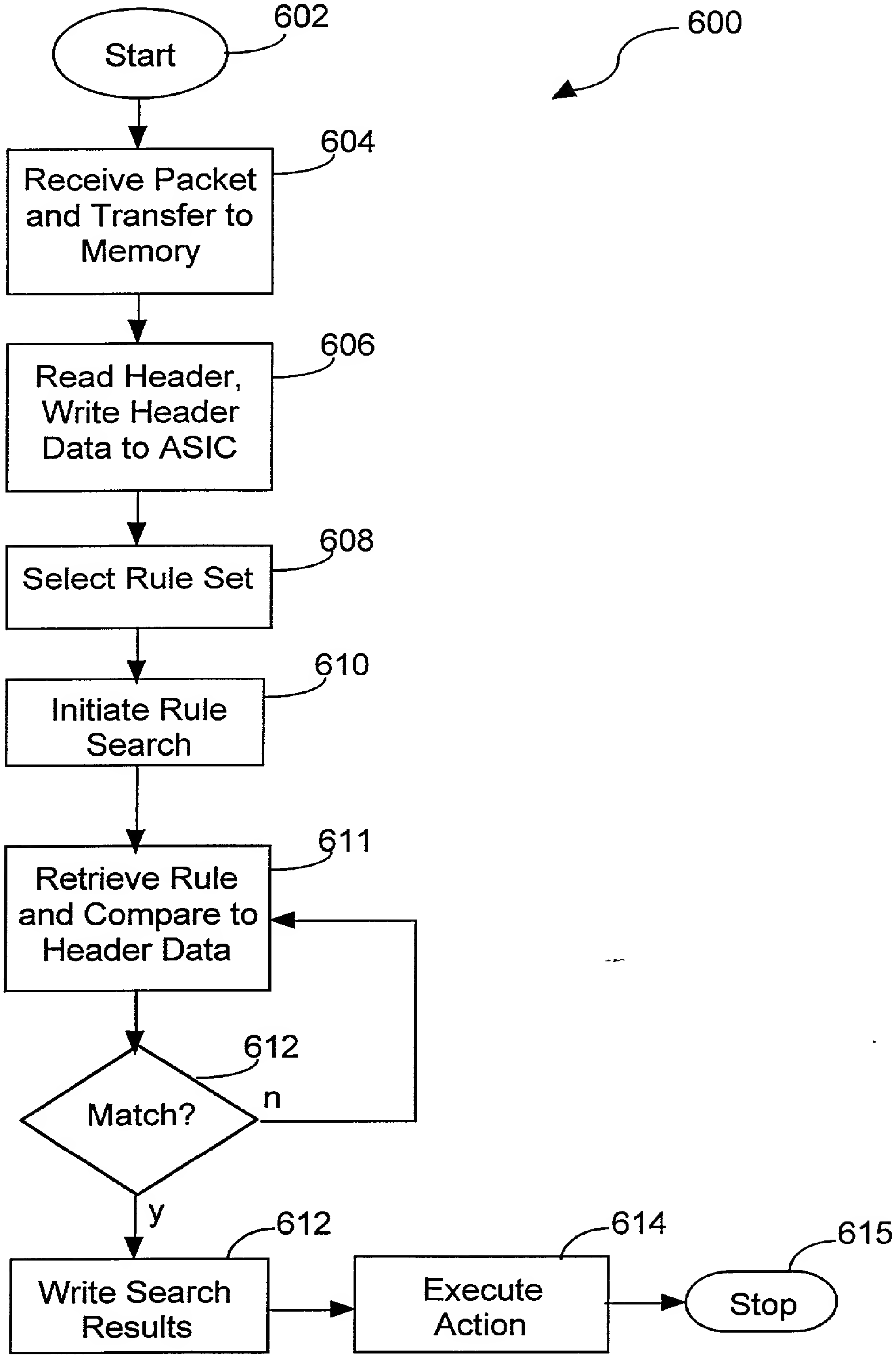
600
Start
602
Receive Packet and Transfer to Memory
604
Read Header, Write Header Data to ASIC
606
Select Rule Set
608
Initiate Rule Search
610
Retrieve Rule and Compare to Header Data
611
Match?
612
n
y
Write Search Results
612
Execute Action
614
Stop
615

FIG. 4

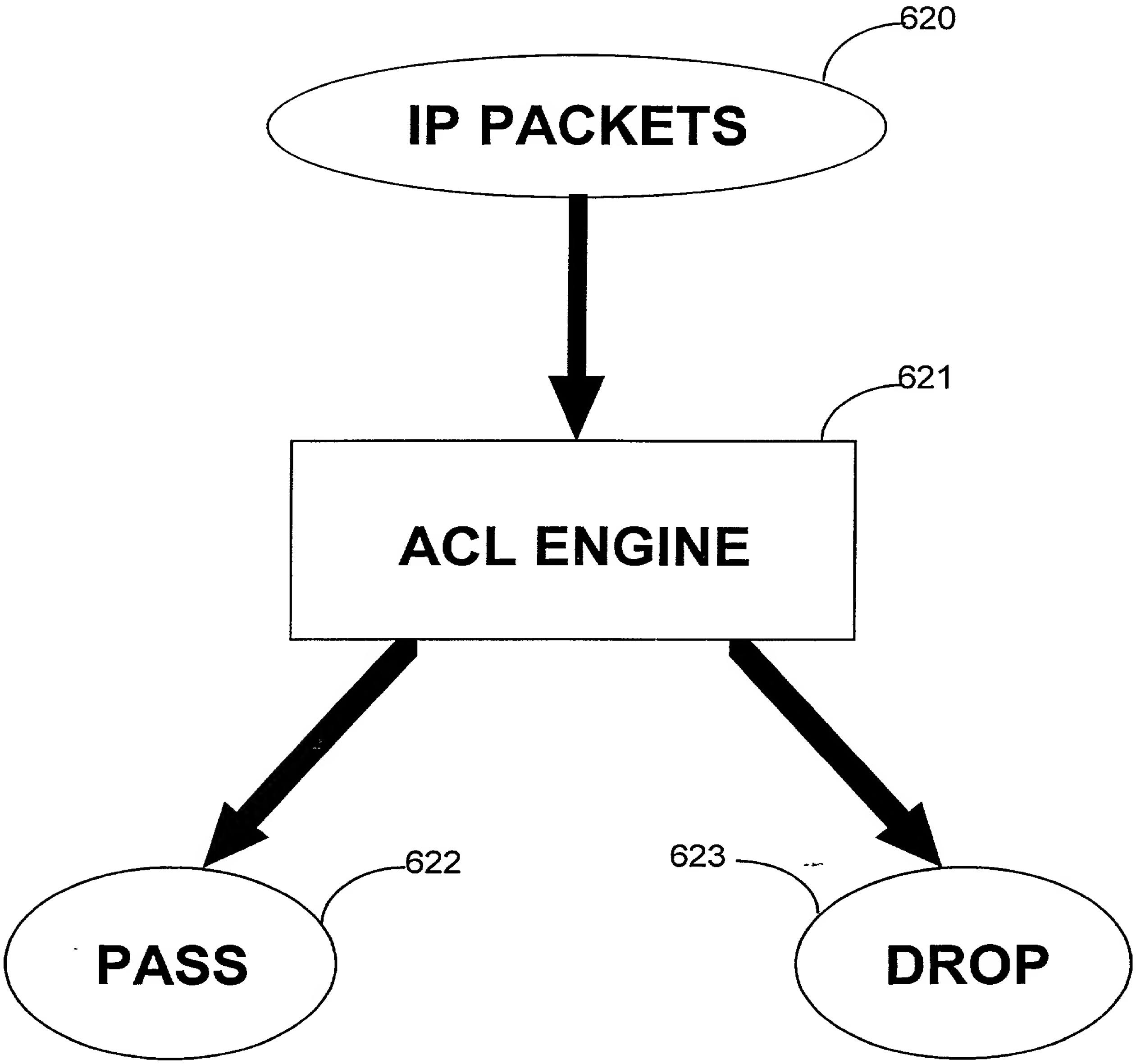

FIG. 5
(Prior Art)

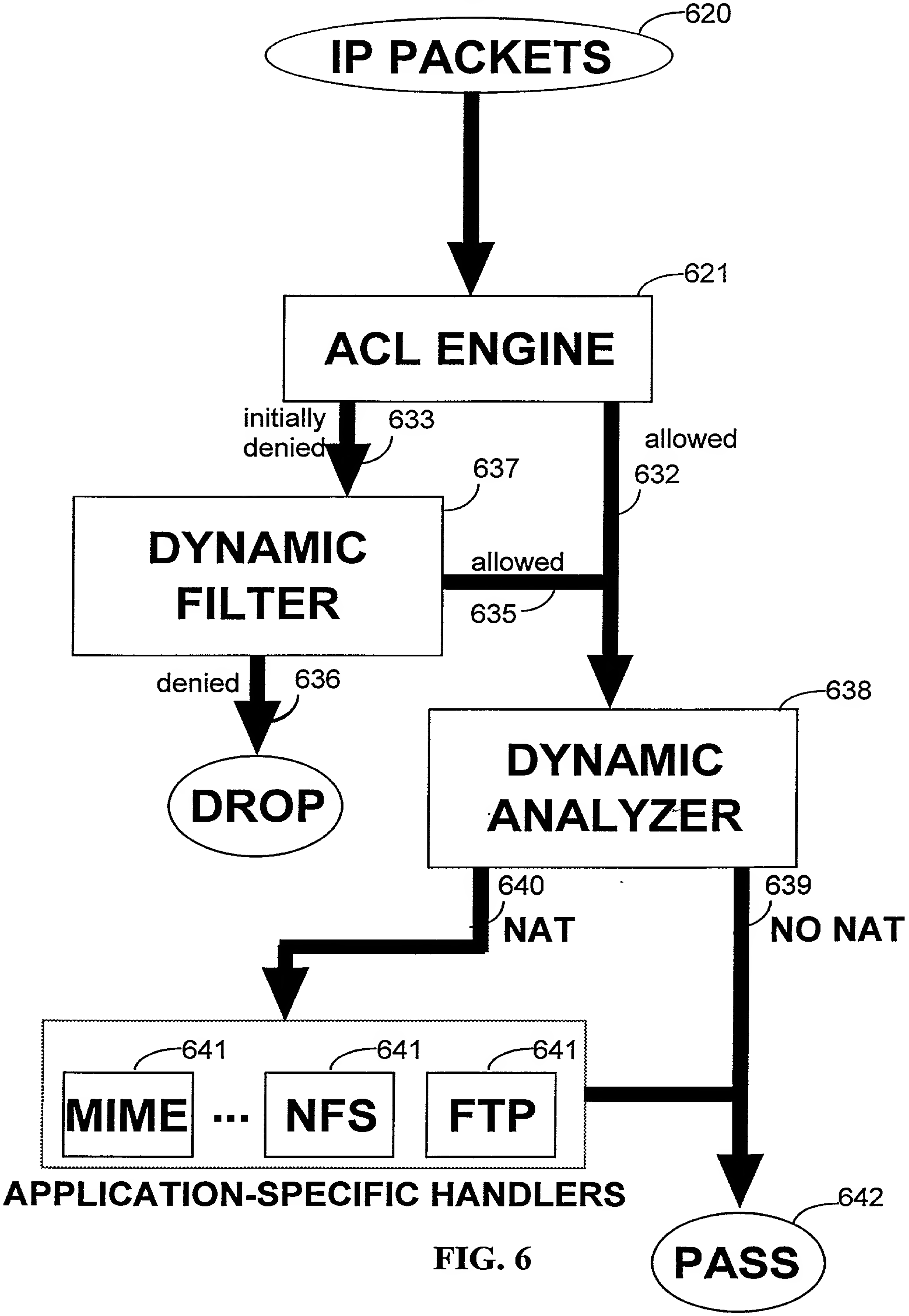
IP PACKETS
620
ACL ENGINE
621
initially denied
633
allowed
632
DYNAMIC FILTER
637
allowed
635
denied
636
DROP
DYNAMIC ANALYZER
638
640
NAT
639
NO NAT
641
MIME
...
641
NFS
641
FTP
APPLICATION-SPECIFIC HANDLERS
PASS
642

FIG. 6

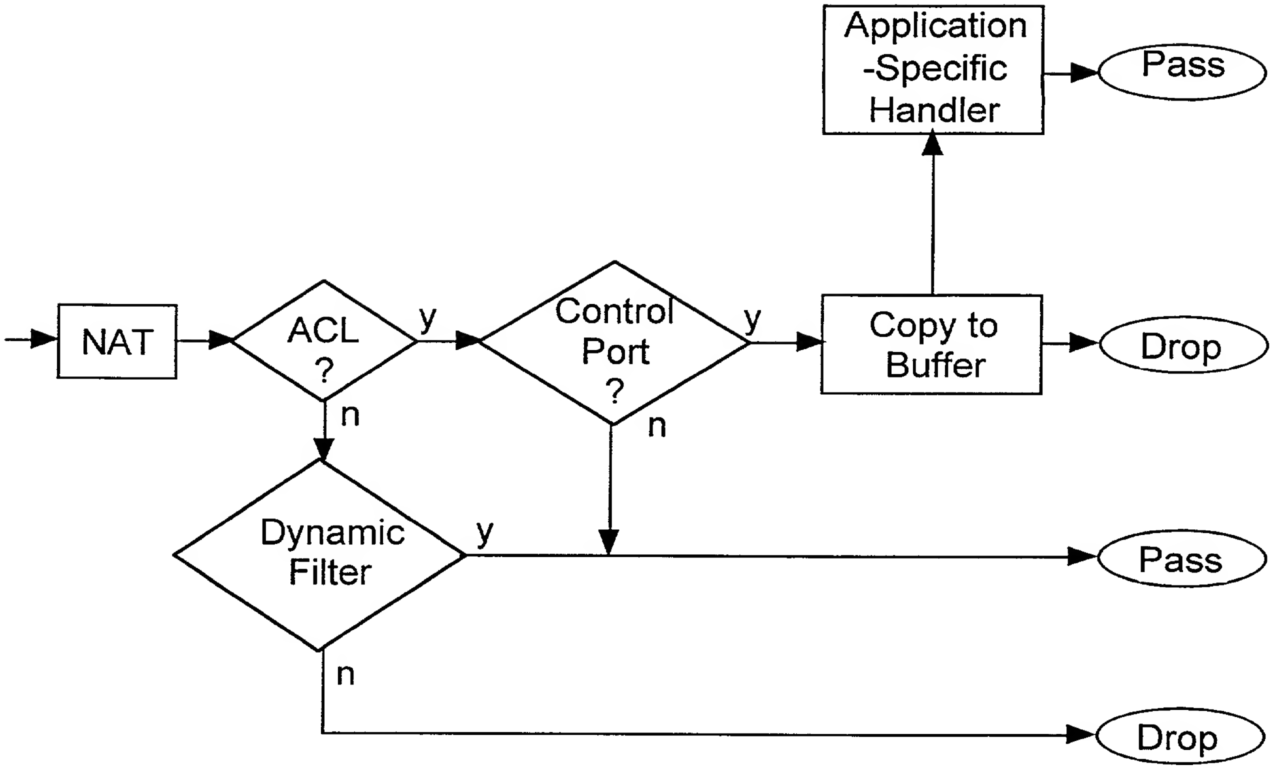
Application
-Specific
Handler
Pass
NAT
ACL
?
y
Control
Port
?
y
Copy to
Buffer
Drop
n
n
Dynamic
Filter
y
Pass
n
Drop

FIG. 7a

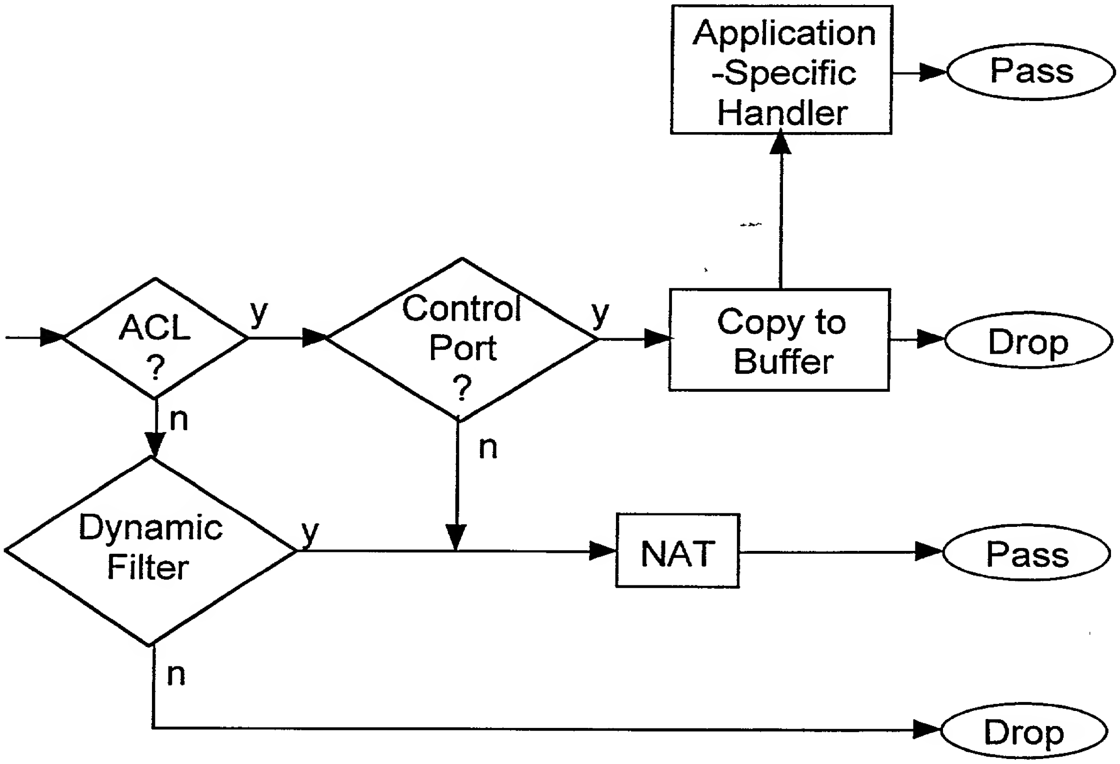
Application
-Specific
Handler
Pass
ACL
?
y
Control
Port
?
y
Copy to
Buffer
Drop
n
n
Dynamic
Filter
y
NAT
Pass
n
Drop

FIG. 7b

DECLARATION
AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below at 201 et seq. underneath my name.

I believe I am the original, first and sole inventor if only one name is listed at 201 below, or an original, first and joint inventor if plural names are listed at 201 et seq. below, of the subject matter which is claimed and for which a patent is sought on the invention entitled

A METHOD, APPARATUS AND COMPUTER PROGRAM PRODUCT FOR A NETWORK FIREWALL

and for which a patent application:
☒ is attached hereto and includes amendment(s) filed on *(if applicable)*
☒ is identified as PENNIE & EDMONDS LLP docket number 9967-003-999
□ was filed in the United States on as Application No. *(for declaration not accompanying application)*
with amendment(s) filed on *(if applicable)*
□ was filed as PCT international Application No. on and was amended under PCT Article 19 on *(if applicable)*

I hereby state that I have reviewed and understand the contents of the above identified application, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119(a)-(d) of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

EARLIEST FOREIGN APPLICATION(S), IF ANY, FILED PRIOR TO THE FILING DATE OF THE APPLICATION			
APPLICATION NUMBER	COUNTRY	DATE OF FILING (day, month, year)	PRIORITY CLAIMED
			YES □ NO □
			YES □ NO □

I hereby claim the benefit under Title 35, United States Code, §119(e) of any United States provisional application(s) listed below.

APPLICATION NUMBER	FILING DATE

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION SERIAL NO.	FILING DATE	STATUS		
		PATENTED	PENDING	ABANDONED
09/283,730	April 1, 1999		X	

POWER OF ATTORNEY: As a named inventor, I hereby appoint S. Leslie Misrock (Reg. No. 18872), Harry C. Jones, III (Reg. No. 20280), Berj A. Terzian (Reg. No. 20060), David Weild, III (Reg. No. 21094), Jonathan A. Marshall (Reg. No. 24614), Barry D. Rein (Reg. No. 22411), Stanton T. Lawrence, III (Reg. No. 25736), Charles E. McKenney (Reg. No. 22795), Philip T. Shannon (Reg. No. 24278), Francis E. Morris (Reg. No. 24615), Charles E. Miller (Reg. No. 24576), Gidon D. Stern (Reg. No. 27469), John J. Lauter, Jr. (Reg. No. 27814), Brian M. Poissant (Reg. No. 28462), Brian D. Coggio (Reg. No. 27624), Rory J. Radding (Reg. No. 28749), Stephen J. Harbulak (Reg. No. 29166), Donald J. Goodell (Reg. No. 19766), James N. Palik (Reg. No. 25510), Thomas E. Friebel (Reg. No. 29258), Laura A. Coruzzi (Reg. No. 30742), Jennifer Gordon (Reg. No. 30753), Allan A. Fanucci (Reg. No. 30256), Geraldine F. Baldwin (Reg. No. 31232), Victor N. Balancia (Reg. No. 31231), Samuel B. Abrams (Reg. No. 30605), Steven I. Wallach (Reg. No. 35402), Marcia H. Sundeen (Reg. No. 30893), Paul J. Zegger (Reg. No. 33821), Edmond R. Bannon (Reg. No. 32110), Bruce J. Barker (Reg. No. 33291), Adriane M. Antler (Reg. No. 32605), Thomas G. Rowan (Reg. No. 34419), James G. Markey (Reg. No. 31636), Thomas D. Kohler (Reg. No. 32797), Scott D. Stimpson (Reg. No. 33607), Gary S. Williams (Reg. No. 31066), William S. Galliani (Reg. No. 33885), Ann L. Gisolfi (Reg. No. 31956), Todd A. Wagner (Reg. No. 35399), Scott B. Familant (Reg. No. 35514), Kelly D. Talcott (Reg. No. 39582), Francis D. Cerrito (Reg. No.38100), Anthony M. Insogna (Reg. No. 35203), Brian M. Rothery (Reg. No. 35340), Brian D. Siff (Reg. No. 35679), and Alan Tenenbaum (Reg. No. 34939), all of Pennie & Edmonds LLP, whose addresses are 1155 Avenue of the Americas, New York, New York 10036, 1667 K Street N.W., Washington, DC 20006 and 3300 Hillview Avenue, Palo Alto, CA 94304, and each of them, my attorneys, to prosecute this application, and to transact all business in the Patent and Trademark Office connected therewith.

SEND CORRESPONDENCE TO:

PENNIE & EDMONDS LLP
1155 Avenue of the Americas
New York, N.Y. 10036-2711

DIRECT TELEPHONE CALLS TO:
PENNIE & EDMONDS LLP DOCKETING
(212) 790-2803

201	FULL NAME OF INVENTOR	LAST NAME XIE	FIRST NAME KEN	MIDDLE NAME	
	RESIDENCE & CITIZENSHIP	CITY Atherton	STATE OR FOREIGN COUNTRY CA	COUNTRY OF CITIZENSHIP United States	
	POST OFFICE ADDRESS	STREET 9 Tuscaloosa Avenue	CITY Atherton	STATE OR COUNTRY CA	ZIP CODE 94027
202	FULL NAME OF INVENTOR	LAST NAME KE	FIRST NAME YAN	MIDDLE NAME	
	RESIDENCE & CITIZENSHIP	CITY San Jose	STATE OR FOREIGN COUNTRY CA	COUNTRY OF CITIZENSHIP Peoples Republic of China	
	POST OFFICE ADDRESS	STREET 6216 Balderstone Drive	CITY San Jose	STATE OR COUNTRY CA	ZIP CODE 95120
203	FULL NAME OF INVENTOR	LAST NAME MAO	FIRST NAME Yuming	MIDDLE NAME	
	RESIDENCE & CITIZENSHIP	CITY Milpitas	STATE OR FOREIGN COUNTRY CA	COUNTRY OF CITIZENSHIP Peoples Republic of China	
	POST OFFICE ADDRESS	STREET 249 Oakhurst Way	CITY Milpitas	STATE OR COUNTRY CA	ZIP CODE 95035
204	FULL NAME OF INVENTOR	LAST NAME	FIRST NAME	MIDDLE NAME	
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP	
	POST OFFICE ADDRESS	STREET	CITY	STATE OR COUNTRY	ZIP CODE
205	FULL NAME OF INVENTOR	LAST NAME	FIRST NAME	MIDDLE NAME	
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP	
	POST OFFICE ADDRESS	STREET	CITY	STATE OR COUNTRY	ZIP CODE
206	FULL NAME OF INVENTOR	LAST NAME	FIRST NAME	MIDDLE NAME	
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP	
	POST OFFICE ADDRESS	STREET	CITY	STATE OR COUNTRY	ZIP CODE

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

SIGNATURE OF INVENTOR 201= KEN XIE	SIGNATURE OF INVENTOR 202- YAN KE	SIGNATURE OF INVENTOR 203- YUMING MAO
DATE 3/14/00	DATE 3/14/00	DATE 3/14/2000
SIGNATURE OF INVENTOR 204	SIGNATURE OF INVENTOR 205	SIGNATURE OF INVENTOR 206
DATE	DATE	DATE

Appendix A